Regulation
on protection, functionality, and quality of IP communications services

CHAPTER I
Objective and scope

Article 1
Objectives

The objective of this Regulation is to enhance consumer protection and strengthen the foundations of the information society by making increased requirements concerning the security of the IP electronic communications services used by businesses and individuals. This Regulation stipulates the measures that the Post and Telecom Administration considers it necessary that electronic communications undertakings adopt in order to guarantee the protection, functionality, and quality of the service rendered. In accordance with the Regulation, there must be measures in place regarding the service, the protection of customer connections, the customer agreements concluded, and the management of the electronic communications networks on which services are rendered, as this is the foundation and premise for effective network service.

Article 2
Scope

This Regulation applies to network and information security falling within the scope of the Electronic Communications Act, no. 81/2003. The Regulation applies to electronic communications undertakings that operate electronic communications services on public communications networks.

They apply to public communications networks and electronic communications services that are transmitted in accordance with IP standards, to and from the customer's equipment. They do not cover the customer's indoor cabling and installations. Internal cabling is discussed separately in the Post and Telecom Administration Regulation on Indoor Cables for Electronic Communications, no. 1109/2006.

This Regulation also applies to the activities of Computer Security Incidents Response Teams (CSIRT) in the electronic communications sector and to electronic communications undertakings' information disclosure requirements vis-à-vis these response teams.

Article 3
Definitions

The words and terms in this Regulation shall mean the following:

Access control: A method for ensuring that only authorised parties have access to an electronic communications network; for example, to defined areas or data, whether these are in electronic form or not.

Availability: Means that data are accessible and services are operational when they are needed, or as possible in cases of power outage, natural disaster, accident, or network attack.

Computer Security Incidents Response Team (CSIRT): A team that works toward safeguarding against security incidents, unstable functionality, and suspicious incidents in information systems and electronic communications networks in Iceland.

Confidentiality: The protection of communications or stored data against interception and reading by an unauthorised person.

Critical infrastructure: The electronic communications network infrastructure that forms the foundation for the electronic communications network as a whole and for the electronic communications services rendered; for example, the innermost core of the electronic communications network and the main network transmission routes, including routes to points abroad. Unstable functionality of such infrastructure could threaten the public's trust in the service rendered by the electronic communications undertaking concerned, and in electronic communications as a whole.

Denial of service: Denial or curtailment of service as a result of interruption, malfunction, or network attack.

Electronic communications network: Transmission systems and, where applicable, switching or routing equipment and other resources that permit the conveyance of signals by wire, radio, by optical or by other electromagnetic means, including networks for radio and television broadcasting and cable television networks.

Electronic communications service: A service that consists wholly or mainly of the conveyance of signals on electronic communications networks, including e-mail services and network access.

Electronic communications undertaking: An individual or legal entity that has notified the Post and Telecom Administration (PTA) of the proposed operation of electronic communications services or an electronic communications network.

Information: Any sort of symbol, signal, writing, image, and sound that is sent or received, and any sort of communication through cables, by radio or other electromagnetic systems.

Integrity: The confirmation that data that have been sent, received, or stored are complete and unchanged.

Internet: An extensive IP electronic communications network that reaches most countries on the globe and is available to all users via diverse IP electronic communications services.

IP electronic communications network: An electronic communications network that transmits data packets in accordance with IP (Internet Protocol) standards.

IP electronic communications services: Electronic communications services that are provided on a public IP electronic communications network, such as e-mail services, web services, name services, file transfer, chat rooms, etc. Also included are operational elements such as domain hosting and IP network registration.

IP network: A series of IP addresses that all conform to the same routing rules; that is, where data packets are directed.

IP transit services: Transit services for IP traffic that an electronic communications undertaking provides via its electronic communications networks through interconnection with another electronic communications undertaking, and where either the recipient or the sender of given data, or neither of them, is a customer of one of the electronic communications undertakings concerned.

Mail server: A mail server to which the customer connects for the purpose of sending e-mail and gaining access to incoming mail in his inbox, among other things. The mail server sends outgoing e-mail to an outgoing mail server, which may be the same server.

Malicious code: Software or programming modules that become lodged in computers and electronic communications networks for the purpose of performing unauthorised or damaging operations. Examples of malicious code are computer viruses and worms.

Malicious traffic: Electronic communications traffic that is sent for the purpose of harming network functionality. Examples of malicious traffic are denial of service attacks and excessive unsolicited bulk e-mail.

Messages: Telephone calls, e-mails, text messages, voice messages, image messages, television programming, IP services, or other comparable message information transferred between parties or to unidentified recipients on an electronic communications network.

Name service: Service that transforms domain names (e.g., www.domain.is) to IP addresses.

Network access: The actual availability of electronic communications networks and related services, including services that authenticate users, identification services, and proxy transfer. It also refers to support services rendered, such as the provision of IP addresses, domains, and web services.

Network and information security: The ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems.

Network attack: An attack launched on an electronic communications network, with the intent to cause denial of services or to interfere with the functionality of networks and systems.

Network termination point: The physical connection point where the subscriber is granted access to a public electronic communications network.

Non-repudiation: A method that ensures that the sender of information cannot deny having sent specific information or that the recipient cannot deny having received it.

Outgoing mail server: Hardware and relevant software that perform the task of forwarding e-mail to the recipient's mail server.

Physical: Refers to a tangible, material item or a real environment.

Proxy transfer: An intermediary in the transfer of customers' electronic communications traffic, which generally hides the registered IP address of the sender and shows instead the intermediary's IP address; for example, so-called proxy service.

Public communications network: An electronic communications network that is used wholly or mainly for the provision of electronic communications services available to the public.

Security event: An identified occurrence of a system, service or network state indicating a possible breach of security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

Security incident: A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Traffic amplification: When traffic is directed along a certain route, which has a multiplicative effect on the traffic to another IP address or hardware.

Web mail server: A mail server to which the customer connects through the mail server's web server.

CHAPTER II
General requirements and instructions

Article 4
General

In all respects other than those stated here, the relevant Post and Telecom Administration Regulation shall apply.

Article 5
Standards

More detailed definitions can be found in the relevant RFC standards from the Internet Engineering Task Force (IETF). In fulfilling the provisions of this Regulation, it is authorised to make use of other technological implementations insofar as these provide equally effective solutions.

CHAPTER III
Network registration and management of IP traffic.

Article 6
General

In order to enhance protection and network service quality, there shall be systematic management of the traffic that transmits the service. Furthermore, it is necessary to enable customers to see the origin of messages.

Article 7
Management and control of public IP traffic

It is necessary to prevent the transfer of unnecessary IP network traffic and routing information between electronic communications undertakings, and to hinder the falsification of IP address origins. The following measures shall be taken, at a minimum:

1. IP traffic to another electronic communications undertaking shall be filtered out if the IP address of the sender is not within the advertised IP address space of the electronic communications undertaking sending the information.
2. It must be ensured that the address of the IP traffic that originates with a directly connected customer is among that customer's allocated IP addresses.
3. An electronic communications undertaking receiving exterior routing updates for IP networks which belong to its own address space shall be filtered out. Exceptions may be made, however, in unusual circumstances where the entities in question so decide – for example in Multi Homing, when one entity connects

to the Internet through two or more other entities along separate paths – for the purpose of increasing transmission security.

4. IP traffic received by an electronic communications undertaking shall be filtered out if the IP address of the sender is among its own IP address space.
5. Electronic communications undertakings shall prevent all types of traffic amplification and other chain reaction of certain traffic to other IP addresses.
6. It is necessary to prevent the transfer of unnecessary route updates and IP traffic between electronic communications undertakings
7. Equipment and routing protocols shall be protected, in the most desirable way possible, against any sort of denial of service or falsified route updates.
8. It is necessary to ensure that false or incorrect route updates of customers' IP networks, such as default route, is not incorrectly advertised on public IP electronic communications networks.
9. Before border routers and routing protocols, which control traffic to another communication undertaking IP communications networks, are set-up or their configuration is changed in any way, they shall always be approved by at least two employees of the electronic communications undertaking concerned, or by a special change management committee appointed by the undertaking for this purpose.
10. Equipment and communications network controls shall be set up so that traffic moves evenly and easily and there are no bottlenecks or hindrances that prevent even transmission functionality in the electronic communications network as a whole, in accordance with the description in the undertaking's business continuity plans.

Article 8

Allocation and registration of IP addresses

Electronic communications undertakings shall assign their customers IP addresses according to specific rules, and enable them to trace the origin of IP traffic and messages through active address registration. The following measures shall be taken, at a minimum:

1. Electronic communications undertakings shall assign their customers IP addresses in accordance with a significant need, and according to the rules of the foreign entity (RIPE-Réseaux IP Européens) that oversees such matters.
2. It must be guaranteed that assigned IP addresses are only used by the customer concerned.
3. The allocation of individual IP addresses or a series of IP addresses shall be carried out without cost to the customer. It is authorised, however, to collect a service charge.
4. An electronic communications undertaking that is peering with or that provides IP transit services to another electronic communications undertaking shall record its routing policy vis-à-vis that undertaking in a public Internet routing registry.
5. The necessary information on the registrants and contact for the IP addresses re-allocated by electronic communications undertakings shall be recorded in the WHOIS regional Internet registry (RIR); including contacts in case of abuse.
6. While a customer has been re-allocated IP addresses from an electronic communications undertaking, he shall retain the registration rights for forward and reverse entries, so long as names are chosen with an eye to general propriety.

CHAPTER IV
Name services

Article 9
General

Measures to guarantee reliability and functionality of name service shall be adopted. Customers must be able to maintain name registration of domains, and pointer records (PTR) for the IP networks allocated to them, so as to make it easier for them to evaluate the quality of the service. Electronic communications undertakings shall not set delegation restrictions on customers if they wish to operate their own name servers and carry out such maintenance there.

Article 10
Registration of domain names

Electronic communications undertakings shall register domains for their customers in the most secure manner possible, and in accordance with the appropriate standards and criteria, including the registration of domains that contain unique Icelandic letters.

Article 11
Registration of pointer records (PTR)

Electronic communications undertakings shall control the registration of pointer records for their own IP networks but shall give their customers the option of controlling PTR registration with their own name servers for the IP networks allocated to them.

Article 12
Protection and functionality of name service

Name servers that customers can look up directly shall only serve a closed group of enquirers; such as, the customers of the electronic communications undertaking concerned. These servers shall be kept separate from the name servers that serve original information on customer domains.

Electronic communications undertakings shall maximise the operational security of name services that store original information by, among other things, placing them on separate IP sub-networks or outside their own IP electronic communications networks.

Name servers shall have sufficient excess capacity that they can best withstand any kind of network attack designed to deny their services. It must be possible to filter out such attacks in a minimum length of time.

Electronic communications undertakings shall guarantee that the name services they provide to protect their records, can confirm the true origin of a reply, and prevent the falsifying of published data in transfer. Name services shall be able to refute the existence of records in a verifiable manner; that is, reply with a message of non-existing record, instead of pointing to another record. Consideration shall be given to the current technology at any given time, and the benefits shall be assessed in comparison with the greater liabilities.

Electronic communications undertakings shall be prepared to restore their name service in the shortest time possible.

Article 13
Monitoring of name services

At a minimum, electronic communications undertakings shall monitor the protection, functionality, performance capacity, and correlation of their name servers. This applies equally to name servers that handle customer queries and to name servers that handle customers' domain names. An attempt shall be made to publicise live results of such measurements to customers, at

least if they do not meet the electronic communications undertaking's requirements according to its business continuity plans.

CHAPTER V
E-mail services

Article 14
General

In order to enhance the quality of e-mail service, operational security measures shall be in place, as shall measures designed to prevent junk mail and/or unsolicited e-mail insofar as is possible. Furthermore, the customer must be able to assess the quality of service and compare the services of various electronic communications undertakings as easily as possible.

Article 15
Protection of e-mail services

Mail servers, equipment that provides proxy transfer, and corresponding equipment managed by electronic communications undertakings shall be protected against being used to forward e-mail without authorisation, for example to send junk mail. Electronic communications undertakings shall test their equipment for this exploitation on a regular basis and shall record the results. They shall also conduct regular testing of the corresponding equipment of their connected customers who operate their own e-mail servers that should only be allowed to forward e-mail traffic originating in their own internal IP communications networks. If the equipment is hosted by another electronic communications undertaking, that undertaking shall carry out the testing.

If a customer´s equipment does not fulfil these requirements, the equipment shall be disconnected from the communications networks until corrections have been made, and the customer shall be notified of these actions.

Electronic communications undertakings shall guarantee the true origin of the e-mail that is sent from their electronic communications networks and shall ensure that their customers' PCs or other equipment cannot be used as tools to send junk mail.

To this end, electronic communications undertakings shall filter-out outgoing e-mail traffic from their customers' networks, to all destination IP addresses on SMTP port 25, with the exception of destination IP addresses of the electronic communications undertakings' specialised e-mail servers and the addresses of agreed hosted e-mail servers within their electronic communications networks. These actions shall take place as close as possible to the customer's connections to the electronic communications network.

If a customer operates his own e-mail server or outgoing mail server, he shall be given the option of having its IP address excluded from filtering out its destination traffic on port 25, even though other IP addresses of that customer are filtered. Furthermore, customers agreed equipment specialised to send solicited bulk mail such as newsletters shall be exempted from this provision.

Customers shall be given the option of sending e-mail through ESMTP port 587 (RFC-4409) to the relevant mail server and outgoing mail server of the electronic communications undertaking, and they shall be encouraged to do so, as well as using SMTP-AUTH (RFC-4954) and encryption; for example, according to the START TLS standard (RFC-4616).

Those customers of an electronic communications undertaking that are temporarily located on the electronic communications network of a third party and are connected to the mail server of that electronic communications undertaking or to a hosted e-mail server on its electronic

communications network, shall only send e-mail through the above-mentioned ESMTP port 587 (RFC-4409) to the e-mail server in question. This port shall not be filtered out in any way in the electronic communications networks. In these instances, electronic communications undertakings shall also authenticate the customer in accordance with recognised RFC standards, such as SMTP-AUTH (RFC-4954) or a corresponding standard. At a minimum, authentication shall be encrypted during transfer to the e-mail server; for example, according to the START TLS standard (RFC-4616).

In their web e-mail servers, electronic communications undertakings shall authenticate their customers and give them the option of encrypting their communications with the web mail server.

Article 16

Further protection and information disclosure

Electronic communications undertakings shall be prepared to activate, in a timely manner, the necessary processes for responding to junk mail that originates in end-users' equipment and in system networking equipment.

Electronic communications undertakings shall monitor mail that is transferred to and from their electronic communications systems, with the objective of detecting unusual e-mail activity and its origins. They shall be prepared to respond accordingly to such incidents.

Electronic communications undertakings shall reject possibly malicious e-mail attachments. If filtering is somehow based on visual inspection of the contents of data, the electronic communications undertakings must receive prior permission from their customers to carry out such filtering.

Electronic communications undertakings shall implement procedures, that allow them to respond effectively to incident reports that are sent between undertakings, and to receive complaints from users.

Electronic communications undertakings shall inform their customers of their security policy and shall provide them with a general description of their security processes.

In order to prevent the delivery of e-mail messages to the wrong party, at least three months must pass before an electronic communications undertaking may re-assign an inactive e-mail address to another customer.

Electronic communications undertakings shall set clear terms and conditions of use for e-mail. They shall also provide their customers with information explaining the risks accompanying junk mail, the measures taken in their electronic communications networks, and the reason why it is important to prevent the abuse of e-mail. Furthermore, they shall advise their customers of useful solutions to protect their computers from abuse of e-mail.

Article 17

Functionality of e-mail service

Electronic communications undertakings shall provide e-mail service in such a manner that functionality is not curtailed significantly as a result of interruptions or malfunctions; for example, by operating failover or dual equipment and implementing load distribution.

In order to distribute the load and reduce the number of interruptions in e-mail service, incoming mail servers shall be kept separate from outgoing mail servers.

Electronic communications undertakings shall be prepared to restore their e-mail service in the shortest time possible.

Article 18

Monitoring of e-mail service

In order to guarantee quality and reliability of e-mail service controlled by electronic communications undertakings, the undertakings shall, at a minimum, monitor the following items and shall inform their customers, in real time, so that they can easily have an overview of the quality of the service:

1. The functional status of the e-mail service.
2. Delays in handling and sending outgoing e-mail from the e-mail systems.
3. Percentage load on the e-mail systems and their e-mail queues.
4. Interruptions in e-mail systems and their history.
5. Operation and functionality of e-mail filters.

E-mail servers and filters that are operated for the particular purpose of handling solicited bulk mail, such as newsletters, are exempted from this provision.

Article 19

Protection against unsolicited bulk mail

Electronic communications undertakings that provide e-mail services shall offer services that protect their customers from unsolicited bulk e-mail or other electronic messages, whether these involve marketing bulk mail or other bulk mail. They shall use measures and technology that are recognised at any given time.

If an electronic communications undertaking becomes aware that its customer sends or forwards such bulk mail over the undertaking's IP electronic communications network, it shall prevent the transfer; for example, by using delayed speed transfer, closure of the port in question, or rejection of the customer's connection.

In general, electronic communications undertakings are authorised to filter out and delete immediately any bulk messages that are clearly flawed and inconsistent with RFC standards. Other messages that the filtering system classifies as unsolicited shall be set aside by the system. The receiving customer shall be notified that he has such messages in storage if he has requested to receive such notification, and they shall be stored for at least six hours before the filter deletes them. It does not matter whether the bulk mail comes from customers of the electronic communications undertaking or from other sources. In their terms and conditions of service, electronic communications undertakings shall inform their customers of their authorisations in this regard.

Easily implemented measures shall be in place if such bulk mail jeopardises the security of critical infrastructure on the electronic communications networks. In such emergencies, it is permissible to resort to more radical measures; for example, filtering out and deleting messages instantly as they arrive in order to protect critical infrastructure, or closing individual system connections. The electronic communications undertaking in question shall then send the Post and Telecom Administration a report on such incidents within 24 hours of their occurrence. The report shall describe the sequence of events, the amount and scope of data deleted, and an assessment of the impact of the incident if these measures had not been taken.

Electronic communications undertakings shall advise their customers on how they can protect themselves from unsolicited mail and where they can direct complaints relative to such unsolicited

mail. It does not matter whether the bulk mail messages originated within or outside the IP communications network of the electronic communications undertaking.

CHAPTER VI
Proxy transfer

Article 20
Traceability

For the purpose of guaranteeing the traceability of the origin of IP electronic communications traffic, the party that provides proxy transfer in electronic communications networks outside its customers' internal communications networks shall deny parties other than its customers to use the service; furthermore, it shall maintain a detailed register of the following each time its customers make use of proxy transfer:

1. From where the data is downloaded or viewed.
2. Customer IP address and customer authentication.
3. The date and time of the communication.

It does not matter whether the equipment is hosted in Iceland or abroad.

Article 21
Information disclosure to customers

In order that customers may be aware of how their electronic communications traffic is transferred, electronic communications undertakings shall provide their customers with information on whether their traffic is sent via proxy transfer, and if so, what traffic is so sent; and whether the proxy transfer is transparent and the limitations it causes, such as possible rejection of traffic and censoring of customer data.

CHAPTER VII
Protection of access connections

Article 22
General

1. It is necessary to prevent the unauthorised redirection of one customer's traffic to another.
2. Electronic communications undertakings shall be prepared to detect and resolve problems in their customer connections that could jeopardise information security and electronic communications network availability.
3. An electronic communications undertaking that sells or delivers pre-setup access equipment to its customers shall protect the equipment against unauthorised electronic communications traffic insofar as is possible; for example, through a firewall installed in an access router, or by having in place effective security measures on wireless local networks. It does not matter whether the customer owns the equipment if the electronic communications undertaking configures it or installs it.
4. Customers must be urged to prevent unauthorised IP traffic in the electronic communications networks and equipment that they install themselves.

CHAPTER VIII
Security incidents and remedies

Article 23
General

It must be guaranteed that communications networks are able to limit the spread of security incidents by, among other things, filtering out undesirable traffic, such as malicious traffic and network attacks that are likely to jeopardise information security and electronic communications network operations.

Article 24
Reporting and management of security incidents

In order to guarantee continuous IP electronic communications services, security incidents and vulnerabilities shall be reported so that it is possible to remedy the situation in a timely manner. Furthermore, it is necessary to guarantee that security incidents are handled in a consistent and efficient manner.

Electronic communications undertakings shall have in place clear and effective procedures for reporting security incidents or the risk of security incidents in their public communications networks as a result of interruptions, failures, changes, and the like. The relevant service criteria shall appear on the undertaking's website or in a comparable medium; for example, in customer agreements. The notification shall state, at a minimum, what effect the incident has or may have, the measures that the electronic communications undertaking intends to take, and advice to customers if such an incident occurs.

Article 25
Co-operation with Computer Security Incidents Response Teams

In order to enhance the integrity and security of electronic communications networks, electronic communications undertakings shall participate in co-operation with Computer Security Incidents Response Teams and co-operation center, whose function is to protect electronic communications networks and information systems in Iceland by, among other things, sending them information on security events, security incidents, interrupted functionality, and suspicious incidents that could cause interruption of continuous service or jeopardise customers' services and data. The Post and Telecom Administration, or the cooperation center that the Administration appoints, shall define what CSIRTs are involved, how the co-operation shall take place, and what information shall be submitted to them.

CHAPTER IX
Service

Article 26
General

A minimum basic level of service must be guaranteed, but it is permissible to provide various service levels in addition to basic service. Customer agreements must be clear, and specified information must be provided to customers so as to facilitate their evaluating the quality of service.

Article 27
Service and agreements

At a minimum, the following shall be included in basic services:

1. At least one IP address.
2. Name service, which consists of at least two separate name servers.

3. Clock service that responds to customer equipment, giving the correct reference clock.
4. IP electronic communications services shall not be delayed unless they jeopardise the electronic communications undertaking's IP networks or cause unusual load at the expense of other IP traffic. In that case, a general notification shall be issued. Furthermore, the electronic communications undertaking shall inform its customers what IP traffic is involved if they request this information. If the delay is persistent, it shall be further described in the terms and conditions.
5. Electronic communications undertakings shall not block their customers' access to the Internet unless this is especially negotiated or is in accordance with this Regulation. Those who seek lawful service shall be enabled to provide equally.

The following shall be offered, either free of charge or for a fee:

1. Users help service, which provides assistance and advice for users of the service.
2. Daily overview of traffic measurement data for the business period if fees are charged according to these measurements, for at least 14 days after the payment due date of the invoice.
3. A further analysis of traffic measurement data, such as the address of source and destination of traffic, from the time that a request to this effect is received.

Basic services shall also include the following in order to facilitate the customer's evaluation of the quality of the IP communication service:

1. Access to a website that enables the customer to measure transmission speed within the IP electronic communications network (for example, TCP performance on port 80), from the customer to the centre of the IP electronic communications network, and from the customer to important border interconnections between the IP communication network and other IP communication networks.
2. A log of those events that affect a large group of customers.
3. Information to the public presented in graphic form, showing the percentage of average load of individual interconnections for the last five minutes; for example, load 50-70%, packet loss less than 0.2%. Also included shall be the undertaking's targets in each instance, which shall apply to the time of day when traffic is heaviest.

Electronic communications undertakings shall make the following information available to their customers so as to enable them to choose the services that best suit them:

1. Information on average packet delay and jitter within the undertaking's individual electronic communications network, including interconnections to abroad.
2. Information on the average response time for the user help service and the average reaction time for failure reports. The undertaking's targets for these shall also be included. If the repair service is divided into regions, the above-mentioned information must be published for each individual region.
3. Information on interconnections with other electronic communications undertakings' IP communications networks.

Article 28

Value added service

Due to the supply of value added service over and above the basic level of service, electronic communications undertakings shall have different elective class of service. These shall be clearly presented so as to enable the customer to purchase the service desired.

At a minimum, the following must appear for all elective class of service:

1. How access to user help service is handled; for example, toll-free number, e-mail address, and hours of operation.
2. How the service level is handled, such as customer's priority to user help service and other support services.
3. Where service is rendered and how access security is handled; for example, whether data are encrypted and where security is provided.
4. Information on other items that is included, such as protection against junk mail, spyware, or undesirable content.

Furthermore, the following must be stated, if appropriate:

1. Whether the customer will be granted access to a service representative.
2. Whether the customer will be granted access to other specialised personnel.
3. Whether the customer will be sent regular reports; for example, on the number of requests for support service, or on the status of systems.
4. Whether the customer is offered an outgoing mail server and information concerning that server.

Article 29

Service web pages

If an electronic communications undertaking grants his customers access to web pages where they can request service or change a request already made, receive information on system status, or take advantage of other options such as using the pages to send messages, they shall limit access to such pages to the party entitled to the service insofar as is possible. At a minimum, the electronic communications undertakings shall set requirements concerning the length and quality of the passwords that provide access to such service pages.

CHAPTER X

Miscellaneous provisions

Article 30

Security audits

The Post and Telecom Administration is authorised to test the protection, functionality, and quality of IP electronic communications services and conduct audits of whether electronic communications undertakings are in compliance with this Regulation. It may carry out such testing and audits on its own initiative or in response to a submitted comment. Testing applies to public electronic communications networks, electronic communications services, and related information systems, among other things. The Administration shall decide how the testing or audits are to be carried out.

The Post and Telecom Administration may decide to engage an independent professional to carry out the audits and submit a report containing the results to the Administration. The auditor shall be obliged to observe confidentiality concerning his work for the Administration. Electronic

communications undertakings shall have the option of commenting on the Administration's choice of auditor.

Article 31
Entry into force
This Regulation shall take effect on 1 July 2008.

Article 32
Authority
The Post and Telecom Administration has issued this Regulation on Protection, Functionality, and Quality of IP Electronic Communications Services pursuant to the authority contained in Article 6 of Act no. 39/2007 Amending the Electronic Communications Act, no. 81/2003.

Post and Telecom Administration, Iceland, 10 December 2007

Hrafnkell V. Gíslason
Björn Geirsson

Section B - Date of issuance: 21 December 2007